CLAIMS

1. A procedure for generating a digital signature with a certification system (8), which encompasses a certification unit (5) and signature (6), characterized in that the certification unit (5) appends information t and authentication information a to the file to be signed, and the supplemented file is signed by the signature unit (6).

2. The procedure according to claim 1, characterized in that the certification unit is a timestamp unit (5), and the information is time information t.

3. The procedure according to claim 1 or 2, characterized in that the signature unit (6) is given intelligent logic via a mobile data carrier.

4. The procedure according to one of claims 1 to 3, characterized in that the authentication information consists of an authentication code a, which is a secret value, for which there is an unambiguous public value a' that cannot be used from outside to infer a.

5. The procedure according to one of claims 1 to 3, characterized in that the authentication code is a digital signature.

6. A device (8) for generating a signature (d) comprising a certification unit (5) and a signature unit (6), characterized in that the certification unit (5) supplies information t and authentication information a.

7. The device (8) according to claim 6, characterized in that the certification unit is a timestamp unit (5), and the information is time information t.

8. The device (8) according to claim 6 or 7, characterized in that the certification unit (5) and signature unit (6) can be separated from each other, and the certification unit (5) is preferably permanently installed and secured against access.

9. The device (8) according to one of claims 6 to 8, characterized in that the signature unit (6) is a mobile data carrier with intelligent logic.

10. The device (8) according to one of claims 6 to 8, characterized in that the signature unit (6) is a plug-in component with storage medium and intelligent logic.